VIRGINIA INFORMATION TECHNOLOGIES AGENCY

REVIEW OF SECURITY CONTROLS
OVER INFORMATION TECHNOLOGY

AUGUST 2005

APA
Auditor of
Public Accounts
COMMONWEALTH OF VIRGINIA

AUDIT SUMMARY

The 2003 General Assembly created the Virginia Information Technologies Agency (VITA) to consolidate information technology efforts in the Commonwealth. One of VITA's main responsibilities is operation of information technology infrastructure for executive branch agencies and the Commonwealth's enterprise systems. Technology infrastructure includes hardware and its associated operating system and resides at VITA's data center and at customer agency locations.

VITA, as its former agency Department of Information Technology (DIT), already operated the Commonwealth's computer data center and the Infrastructure of the Commonwealth's enterprise systems. However, the responsibility for infrastructure residing at the executive agencies is new. This report reviews VITA's policies and procedures placed in operation as of July 15, 2005.

We found:

- VITA has not yet developed or implemented policies, procedures, or standards for information systems infrastructure. VITA is responsible for operating and providing security for most executive agencies, however, VITA employees are currently following customer agencies' policies and procedures. VITA has not reviewed or approved these agencies' policies, procedures, and standards, and therefore, does not know if they are sufficient to provide proper security;

- VITA has not completed updating Memorandum of Agreements (MOAs) with customer agencies that use the VITA server farm. Many MOAs were written before VITA's creation and do not reflect VITA's security responsibility. These MOAs are vague and do not clarify security responsibilities. Adding to the confusion, VITA does not maintain documentation for requests and approvals to variations from policy, procedures, and standards in the Windows environment of the server farm. In addition, VITA could not provide us with documentation for some variations in the UNIX environment of the server farm;

- VITA lacks documentation of policies, procedures, and standards for routers and firewalls located at the data center. Although these devices appeared to be configured securely at the time of our review, without policies, procedures, and standards, VITA cannot ensure that the configurations are consistent or that changes to configurations conform to management's required level of security; and

- VITA updated its Risk Assessment and Business Impact Analysis in June. These documents identify critical and confidential resources and their associated risks, but do not reflect VITA's responsibility for infrastructure outside of the data center. Without these documents, VITA cannot ensure controls are in place to reduce identified risks and cannot ensure that the business recovery plan is sufficient to restore critical operations.

-TABLE OF CONTENTS-

INTRODUCTION

The 2003 General Assembly created the Virginia Information Technologies Agency (VITA) to consolidate information technology efforts in the Commonwealth. The creation of VITA encompassed combining three existing information technology agencies: the Department of Information Technology (DIT), Department of Technology Planning, and the Virginia Information Providers Network, and transferring personnel, equipment, and technology infrastructure from individual executive branch agencies to VITA.

One of VITA's main responsibilities is operation of information technology infrastructure for in-scope executive branch agencies and the Commonwealth's enterprise systems. Technology infrastructure includes hardware and its associated operating system. VITA, as its former agency Department of Information Technology, already operated the Commonwealth's computer data center and the infrastructure of the Commonwealth's enterprise system. However, the responsibility for infrastructure residing at executive agencies is new.

This report is a review of the security controls VITA has put into place over their information technology infrastructure. The objectives of our review were to determine whether VITA developed and follows policies and procedures to provide reasonable assurance that:

- only properly authorized individuals have logical access to programs and data in the MVS and UNISYS environments;
- data completeness and security occurs for data transmissions/communications between VITA and its customers;
- proper authorization, testing, approval, implementation, and documentation occur for changes to hardware and software;
- the VITA server farm has proper logical controls in place;
- VITA has a current Risk Assessment, Business Impact Analysis, and Disaster Recovery Plan; and
- policies, procedures, and standards exist for VITA operations at customer agency locations.

The Auditor of Public Accounts determined the nature, timing, and extent of tests performed in order to obtain evidence about the operating effectiveness of VITA's policies and procedures in meeting specified control objectives. We have defined the control objectives for this review from the Information Systems Audit and Control Foundations work on "Control Objectives for Information and Related Technology" (COBIT). COBIT represents generally applicable and accepted standard for good practices for information technology.

OVERVIEW OF SERVICES PROVIDED

VITA provides the Commonwealth of Virginia with a means of meeting its information technology needs. VITA manages the state's telecommunications contracts; provides state government with data processing services; assists state agencies and local governments with designing and purchasing information technology resources; and provides other information technology services, such as audio and video conferencing.

VITA offers data processing services through the operation of the state data center. The data center houses mainframes and servers supporting MVS, UNYSIS, UNIX, and Windows NT operating environments. These systems operate many of the state's critical systems, including the Commonwealth's Accounting and Reporting System, the Commonwealth's Personnel Management System, the Department of Motor Vehicles' Customer Service System, and the Department of Social Services' Child Support System. In addition, VITA houses a server farm with UNIX and Windows NT servers. The server farm provides agencies a place to physically store critical servers. The server farm also contains web page servers for many of the Commonwealth's agencies.

In addition, VITA is responsible for the operations and security of most hardware and operating systems for in-scope agencies. This includes many different types of equipment and technologies.

AREAS OF REVIEW

MVS and UNISYS Environments

Our first objective was to ensure policies and procedures provide reasonable assurance that only properly authorized individuals have logical access to programs and data in the MVS and UNISYS environments. In meeting this objective, we reviewed policies and procedures related to granting, terminating, and modifying user's access to the MVS and UNISYS environments. We also tested compliance with the policies and procedures.

In the MVS environment, VITA controls logical access to data and programs through the ACF2 security package. VITA establishes user accounts in the operating system; however, the operating system default allows access to all programs. To mitigate this weakness, VITA uses ACF2 to provide security to all programs except some specific IMS programs. VITA sets up the ACF2 logon and customer agencies must prepare specific rules to allow user access to programs.

Customer agencies appoint an Agency Security Officer, who establishes, maintains, updates, and deletes access for customer agency end-users. To establish or make changes to a logon, the customer agency must complete a form for each individual user. The Agency Security Officer, VITA Security Officer, System Coordinator, and Direct Access Storage Device Coordinator must sign the form indicating approval. After receiving the form, VITA verifies the Agency Security Officer signature, confirms for new logons that the requested logon meets specific character requirements and does not exist, and then completes the request.

Our review of the MVS environment included interviewing personnel and reviewing policies and procedures to gain an understanding of how VITA uses ACF2 and verifying whether VITA establishes appropriate global settings and access to critical data sets. We also gained an understanding of the security reports VITA uses for controlling access. In addition, we reviewed VITA employees' access and logons to determine if security privileges are appropriate and access provides the least privilege to perform job duties. We reviewed terminated employee logons to ensure timely deletion. Finally, we reviewed access request forms to ensure VITA obtained all required approvals.

The results of our review revealed that VITA has sufficient policies and procedures concerning logical access to the MVS environment. In addition, we noted no exceptions to policies and procedures in our test work.

In the UNISYS environment, VITA provides three types of security for protecting customer agency data and programs: (1) Read-Write Access; (2) Access Control Records (ACR); and (3) Compartments for protecting customer agency data. VITA recommends, but cannot mandate that customer agencies use these security features. If an agency does not use one of the security options, then other UNISYS customers have free access to the computer programs and data.

Each customer agency must select a UNISYS sub-administrator and send a letter to VITA indicting the sub-administrator's name to establish the appropriate security access. VITA does not set up access for any of the customer agency's employees except the sub-administrator. The customer agency implements procedures for setting up and maintaining end-user logon ID's and privileges.

UNISYS environment audit test work involved gaining an understanding through interviews and review of policies and procedures of how VITA administrates and uses the environment. We also reviewed sub-administrator access request forms for proper approval and submittal through appropriate channels. Beyond sub-administrators, user access is the responsibility of customer agencies.

We determined VITA has sufficient policies and procedures concerning logical access to the UNISYS environment.

Telecommunications

Second, we determined whether VITA's policies and procedures provide reasonable assurance that data completeness and security occurs for data transmissions/communications between VITA and its customers. Customer agencies can gain computer communication access through VITA through a variety of state telecommunications agreements, including the COVANET contract, Verizon contract, Network Virginia, or several other agreements with local exchange carriers.

COVANET is a state contract that provides statewide data services dedicated to the Commonwealth of Virginia using MCI's commercial network. The backbone network is not exclusive to the Commonwealth, but is a network accessed by MCI's commercial and corporate customers. Agencies can use COVANET as a private network backbone or as their gateway to the Internet. Additionally, Verizon provides statewide data services to the Commonwealth of Virginia. Agencies can use Verizon as a private network backbone or as their gateway to the Internet. Lastly, Network Virginia is a statewide network primarily used by Commonwealth of Virginia colleges and universities, as well as local government, public schools, and private businesses.

Customer agencies contact VITA to establish the proper connections to send data. VITA contracts with the various communications companies to provide the requested telecommunication service. The telecommunications companies, such as MCI, Bell Atlantic, and Sprint, own and control the physical lines from the customer agency to VITA. VITA takes no responsibility for these lines.

VITA has one main router to control and direct traffic from COVANET and Network Virginia. VITA configures its router to allow traffic coming in from the Intranet to only access VITA's web page and the DNS server that provides various state agency home page information. The router table configuration includes an access list of customers that need to access the mainframe systems and servers at VITA through COVANET and Network Virginia. The access list is a security feature programmed into the router using Internet Protocol (IP) addresses. Only customer agencies using the specified IP address can gain access through the router.

Once through the router, VITA firewalls provide an additional security barrier by blocking external networks from accessing VITA's computer environment. At the time of our test work, VITA operated

17 firewalls at their data center. Customer agencies request access through the firewall to access the VITA systems. The Agency Security Officer requests access by contacting the VITA Help Desk and completing a firewall access form. The VITA firewall administrator then establishes the access based on IP addresses.

In meeting this objective, we reviewed policies and procedures and interviewed appropriate staff to gain an understanding of VITA's network environment, including the firewall and routers. We also determined whether VITA reviewed monitoring reports generated by these devices. Finally, we obtained and reviewed configuration files for a sample of routers and firewalls to determine if VITA ensured proper authorization of users and disabled risky services.

Our review found that VITA does not have written policies and procedures governing their routers and firewalls. Although we did not note any weaknesses in the current settings, documenting the policies, procedures, and standard configurations ensures the consistent application of security controls. Policies and procedures should include at a minimum: staff requirements; monitoring and logging procedures; granting, modifying, terminating, and reviewing access procedures; and a standard baseline configuration. VITA should document policies, procedures, and standards governing their routers and firewalls.

Change Management

Change management controls are important to ensure the reliability, availability, and effectiveness of systems and data. Our objective for change management was to determine whether VITA's policies and procedures provide reasonable assurance that proper authorization, testing, approval, implementation, and documentation occur for changes to existing system software and implementation of new systems. VITA defines a change as any alteration to any component of the VITA infrastructure of hardware, software, facilities, network communications, procedures, scheduling process, or system documentation. We reviewed VITA's policies and procedures for change management and selected a sample of changes to ensure compliance.

Per the policies and procedures, all changes start with a change request submitted to VITA's Change Management System, Applix. The requestor's manager or supervisor must first approve the change, and then send it to the appropriate Operations Analyst for review. After review, the Ops Analyst presents all planned changes at a weekly change management meeting. All individuals involved in the change must attend the meeting or send representation. This meeting is the final approval for the change request. If the change is approved, an engineer or technician completes the requested change and the change requestor indicates the completion or incompletion of the change by checking a box in the Applix application.

Our review found VITA's policies and procedures do not require engineers test changes in a test environment or document a rollback plan before placing changes into production. We also noted that the requestor and engineer are often the same person for hardware changes. When this is the case, VITA does not require a second technical review of the completed change. In our sample of changes, we found these items inconsistently documented and performed.

The lack of testing could lead to changes in the environment, which disrupt operations, compromise security, or corrupt data. Rollback plans should document steps to facilitate an efficient reversion to the system's original state and minimize the risk of lost of data in case of failure during implementation. Finally, high risk changes should undergo a soundness review by another technical resource to ensure the change works as intended and meets the business need. We recommend VITA modify policies and procedures related to high risk changes to include testing of changes in a test environment before implementation into production, documentation of a roll back plan, and a technical review after implementation.

Server Farm

Our fourth objective determines whether VITA established and follows policies and procedures to provide reasonable assurance that the VITA server farm has proper logical controls in place. The server farm consists of UNIX and Windows servers, which were owned by customer agencies before the transition. VITA establishes MOAs to document the agreed-upon level of service between VITA and the agency requesting use of the farm. VITA currently has MOAs with the Departments of Social Services and Taxation, Virginia Employment Commission, and Virginia Retirement System. In addition, the server farm houses servers, which provide web site hosting for approximately 47 agencies, localities, boards, or commissions.

We reported in last year's VITA SAS 70 audit report that the lack of detailed security information in the MOAs requires VITA to take steps to avoid miscommunication of roles and responsibilities of each party. With the transition to VITA, the servers became the property of VITA and responsibilities became even more complicated. VITA has not updated most MOAs to clearly define the security responsibilities.

Our review of the server farm consisted of gaining an understanding of roles and responsibilities based on MOAs in place and reviewing policies, procedures, and standard configurations. We found VITA had standard configurations for their Windows and UNIX servers. We then reviewed the security settings on a sample of the UNIX and Windows servers in the server farm to determine compliance with policies and procedures and establishment of proper logical security controls.

In addition to the lack of updated MOAs, we found that VITA does not maintain documentation of the request and approval for some exceptions to the server configuration policies. The audit team could not clearly determine who requested or approved exception to the policies for both the UNIX and Windows servers.

We recommend VITA update all MOAs with server farm customers to clearly reflect responsibilities and policies, procedures, and standards. VITA should also ensure it documents all requests and approvals for exceptions to policy.

Business Impact, Risk Assessment, and Recovery

A Business Impact Analysis and Risk Assessment identifies information resources that are confidential and critical and the potential security threats and risk to those resources. Based on the results of these documents, an entity develops a business recovery plan to define maximum allowable downtime and document plans for restoration of critical resources. We reviewed VITA's business impact, risk assessment and recovery plans to determine if these documents reflected VITA's current operating environment and responsibilities. Our review found that VITA's risk assessment and continuity plan does not incorporate enterprise infrastructure. VITA updated their data center risk assessment in June 2005; however, without including infrastructure, the documents are not complete. Without a complete business impact or risk assessment, VITA cannot ensure controls in place to mitigate identified risks and ensure the business recovery plan is complete.

VITA does not have a plan to develop a complete risk assessment or continuity plan. However, VITA is currently working on a project which would help them develop a risk assessment. VITA contracted with a consulting company to perform risk assessments on in-scope agencies based on questionnaires. We encourage VITA to use the results of the security assessments to develop a complete risk assessment for all VITA's assets acquired during transition. After completion of these documents, VITA should ensure their disaster recovery plan reflects the results of the Business Impact Analysis and Risk Assessment. We encourage VITA to complete these documents as quickly as possible.

Customer Locations

As of January 2005, VITA owns and operates all in-scope executive agencies' technology infrastructure. This responsibility includes the acquisition, operation, and maintenance of local and wide area network and application servers, computer rooms, voice and data communications, desktops, laptops, portable devices, and peripherals. In support of this responsibility, most in-scope agencies information technology employees transferred employment to VITA.

The transition of in-scope agencies to VITA occurred in three phases based on agency size. The transition started in 2003 and ended December 31, 2004. During that time, in-scope agencies transferred ownership of hardware and employee positions to VITA. However, VITA left employees in the same positions and is exercising insufficient authority over the operations or security of the newly acquired hardware and staff. As a result, VITA employees continue to operate under the customer agencies policies and procedures.

In July 2005, we surveyed the 17 agencies, which have activities that would have a material impact on the Commonwealth's Annual Financial Report or Statewide Single Audit. The purpose of the review was to determine which policies and procedures these agencies use to secure and operate their infrastructure. We found that VITA has not yet developed or issued policies and procedures for the operation of VITA owned infrastructure located at customer agency locations. VITA employees at each location are still following the customer's policies and procedures, which vary at every location. VITA has not reviewed those policies and procedures and does not know if they are sufficient to protect VITA resources and their customer's data.

We recommend VITA develop policies, procedures, and standards for the operation of infrastructure. Policies and procedures will communicate management's standards for operation and security of infrastructure. By not having these policies and procedures, VITA employees are left to determine their own level of operational effectiveness and security and for accepting risks for which VITA management is unaware.

RECOMMENDATIONS SUMMARY

Develop Policies, Procedures, and Standards for Infrastructure

VITA has not yet developed or implemented policies, procedures, or standards for information systems infrastructure. VITA is responsible for operating and providing security for most executive agencies' computing infrastructure; however, VITA employees are currently following customer agencies' policies and procedures. VITA has not approved these agencies' policies, procedures, and standards and does not know if they are sufficient.

Additionally, VITA does not have documented policies, procedures, and standards for routers and firewalls at the data center. The routers and firewalls protect critical and confidential Commonwealth data. Without the policies and procedures, VITA cannot ensure a consistently secure environment.

Policies, procedures, and standards provide direction and a baseline for employees to implement the controls management determined necessary to protect their resources. Without polices, procedures, and standards, VITA employees are left to set their own direction and determine which risks to accept. Failure to implement proper policies, procedures, and standards could allow the loss of confidentiality, integrity, or availability of critical data and resources.

VITA should develop and implement policies, procedures, and standards for common infrastructure elements. VITA should review the policies, procedures, and standards with customer agencies and VITA security should approve any exceptions in writing. Since VITA is ultimately responsible for the security of infrastructure, they should have the final say in approving exceptions.

Update MOAs and Maintain Documentation for Exceptions to Server Policies

VITA does not have current MOAs for most server farm customers and does not maintain documentation of requests and approvals for all Windows and some UNIX server exceptions to configuration procedures and standards. Most MOAs enforced at the server farm are those written before the creation of VITA and do not reflect VITA's new security responsibilities. Adding to the confusion, the audit team could not clearly determine who requested or approved exceptions to the policies regarding the servers located in the server farm.

Management develops policies and clearly communicates responsibilities to encourage compliance with internal controls and reduce risk. Exceptions to policies represent a higher level of risk, so when they occur it should be clear which manager approved the change. This approval provides a source of risk acceptance and accountability for any departure from policy.

We recommend that VITA update all MOAs with its customers to reflect current responsibilities and policies, procedures, and standards. Also, VITA should fully document the requests and approval of exceptions to agreed-upon policies, procedures, and standards. The above recommendation will strengthen the awareness and approval of potential risks for VITA and the customer.

Improve Policies and Procedures over Change Management

VITA's policies and procedures do not require engineers to test changes in a test environment or to document a rollback plan prior to implementation. Additionally, VITA's policy requires the requestor to review completed changes; however, for hardware changes, the requestor and engineer are the often the same person. When this is the case, there is no review of the completed change by someone other than the engineer.

The lack of testing could lead to changes in the environment, which disrupt operations, compromise security, or corrupt data. Technicians should document rollback plans for each change to minimize the risk of lost data and facilitate an efficient reversion to the system's original state in case of failure during the change. Finally, another technical resource should review high risk changes for soundness to ensure the change works as intended and meets the business need.

VITA management should modify existing change management policies and procedures to include a documented and approved rollback plan, procedures for testing changes, and procedures for review of completed high risk changes.

Complete Business Impact and Risk Assessment

VITA does not have a complete business impact or risk assessment including executive infrastructure. The business impact and risk assessment identifies information resources that are confidential and critical and the potential security threats to those resources. Without a risk assessment, VITA cannot ensure controls are in place to protect critical assets against identified risks.

We encourage VITA to use the in-scope agency security assessments to update its risk assessment and business impact analysis as quickly as possible. VITA should then use these documents to ensure controls are in place to reduce identified risks and a business recovery plan is in place to restore critical assets in the event of disruption of operations.

Commonwealth of Virginia

Auditor of Public Accounts
P.O. Box 1295
Walter J. Kucharski, Auditor
Richmond, Virginia 23218

July 15, 2005

The Honorable Mark R. Warner
Governor of Virginia
State Capitol
Richmond, Virginia

The Honorable Lacey E. Putney
Chairman, Joint Legislative Audit
and Review Commission
General Assembly Building
Richmond, Virginia

We have completed our audit of the internal controls within the Virginia Information Technologies Agency (VITA) to determine if they are sufficient to provide accurate financial information for the compilation of the Commonwealth's Comprehensive Annual Financial Report and Statewide Single Audit. We conducted our audit in accordance with the standards for performance audits set forth in Government Auditing Standards, issued by the Comptroller General of the United States.

Audit Objectives

The objectives of our audit were to determine whether VITA's policies and procedures provide for adequate controls over security of their customer systems and whether VITA is following the policies and procedures.

Scope and Methodology

In conducting our review, we considered the traditional services offered by VITA, which are generally located at VITA central, and new services offered at customer locations. We reviewed VITA's policies and procedures; interviewed appropriated personnel; reviewed documents, records, and system's settings; and performed such other auditing procedures as we considered necessary to achieve our objectives. Our review included controls over the mainframe, server farm, and network operations at VITA central. We planned to review VITA controls at customer locations; however, we found that the controls at the customer sites were not VITA controls.

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered materiality and control risk in determining the nature and extent of our audit procedures. We performed audit tests to determine whether VITA's controls were adequate, had been placed in operation, and were being followed.

Management has responsibility for establishing and maintaining internal control and complying with applicable laws and regulations. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations.

Our audit was more limited than would be necessary to provide assurance on internal control or to provide an opinion on overall compliance with laws, regulations, contracts and grant agreements. Because of inherent limitations in internal control, errors, irregularities, or noncompliance may nevertheless occur and not be detected. Also, projecting the evaluation of internal control to future periods is subject to the risk that the controls may become inadequate because of changes in conditions or that the effectiveness of the design and operation of controls may deteriorate.

The description of specific policies and procedures at VITA and their effect on assessments of control risk at customer organizations are dependent on their interaction with the policies, procedure, and other factors present at individual customer organizations. We have performed no procedures to evaluate the effectiveness of policies and procedures at individual customer organizations.

This report is intended for the information and use of the Governor and General Assembly, management, and citizens of the Commonwealth of Virginia and is a public record.

We discussed this letter with management at an exit conference held on September 7, 2005.

AUDITOR OF PUBLIC ACCOUNTS

KSA/kva

COMMONWEALTH of VIRGINIA

Lemuel C. Stewart, Jr.
CIO of the Commonwealth
Email: lem.stewart@vita.virginia.gov

Virginia Information Technologies Agency
110 South 7th Street
Richmond, Virginia 23219
(804) 371-5000

TDD VOICE -TEL. NO.
711

September 13, 2005

Mr. Walter J. Kucharski
Auditor of Public Accounts
Post Office Box 1295
Richmond, Virginia 23218

Dear Mr. Kucharski:

Thank you for the opportunity to respond to the Auditor of Public Accounts' audit of the Virginia Information Technologies as of July 15, 2005. Your review comes about six months after VITA's completed integration of all in-scope agencies' IT infrastructure, staff & operations and highlights some of the challenges we face with our combined and inherited environments.

We are in agreement with your four recommendations and will prepare a recommended corrective action plan accordingly for consideration and adoption by the Finance and Audit Committee and the Board at their October meetings. In fact, efforts are and have been underway in most areas. As always, we appreciate the professionalism of your staff.

Sincerely,

Lemuel C Stewart Jr

Lemuel C. Stewart, Jr.

c: The Honorable Eugene J. Huang, Secretary of Technology
Judy Napier, Assistant Secretary of Technology
Members, Information Technology Investment Board